MANUAL DE INSTALAÇÃO E CONFIGURAÇÃO

Utilização do Certificado Tipo A3 Com Navegador Mozilla Firefox 35.0.1

As informações contidas neste documento não podem ser reproduzidas sem a expressa permissão da Certisign.

Controle de Revisões

Tabela 1: Controle de alterações do documento

Nome do responsável	Assunto/ Motivo	Versão	Data
Michele Catiuze M Santos	Manual de Utilização do Certificado Tipo A3	1.0	04/02/2015
Equipe Qualidade e Segurança de SW	Revisão do Documento	1.2	11/02/2015

Sumário

1. Introdução 3
2. Pré-Requisitos 3
3. Instalação do SafeNet Authentication Client 9.0.43.0 4
4. Utilização do Certificado A3 no Navegador Mozilla Firefox 35.0.1. 9
5. Teste o Certificado Digital. 15

As informações contidas neste documento não podem ser reproduzidas sem a expressa permissão da Certisign.

1. Introdução

Com a rápida adoção do uso de certificados da ICP-Brasil pelo governo Brasileiro, nas relações com os cidadãos à disponibilização da possibilidade de uso dos certificados digitais armazenados em mídias criptográficas em sistemas operacionais MAC OS desenvolvidos pela empresa Apple, se faz necessária, e buscando atender as necessidades de nossos clientes a CERTISIGN vem trabalhando junto com seus fornecedores para disponibilizar os drivers necessários para o funcionamento dos dispositivos criptográficos nesse sistema operacional.

Este manual tem o objetivo de apresentar os mecanismos e processos necessários para permitir que sejam instalados e disponibilizados para uso, em mídias criptográficas comercializadas com os certificados digitais e-CPF, e-CNPJ e NF-e da Certisign.

2. Pré-Requisitos

É imprescindível que os procedimentos mencionados abaixo sejam realizados ***com mídia criptográfica conectada na máquina*** desde o inicio da configuração e instalação.

Antes de iniciar o processo de configuração, favor fechar todas as aplicações.

Se você tiver alguma versão anterior do SafeNet Authentication Client instalada no seu computador, remova, reinicie o computador e instale a versão SafeNet Authentication Client 9.0.43.0.

Os usuários precisam ter privilégios de administrador para instalar a CSP – Cryptographic Service Provider. Caso você não seja administrador da sua máquina entre em contato com o responsável pela infraestrutura de sua empresa.

Necessário ter instalado o Navegador Mozilla Firefox 35.0.1 na máquina.

As informações contidas neste documento não podem ser reproduzidas sem a expressa permissão da Certisign.

3. Instalação do SafeNet Authentication Client 9.0.43.0

Para iniciar o processo de instalação do SafeNet é necessário realizar o download do arquivo ***SafeNet AuthenticationClient 9.0.43.0.dmg***, que é disponibilizado no site da Certisign através da área de suporte.

(*https://www.certisign.com.br/atendimento-suporte/downloads/tokens/mac*)

É recomendado que o arquivo seja salvo na Mesa de Trabalho do Mac OsX para facilitar a sua localização, conforme a Figura 1:

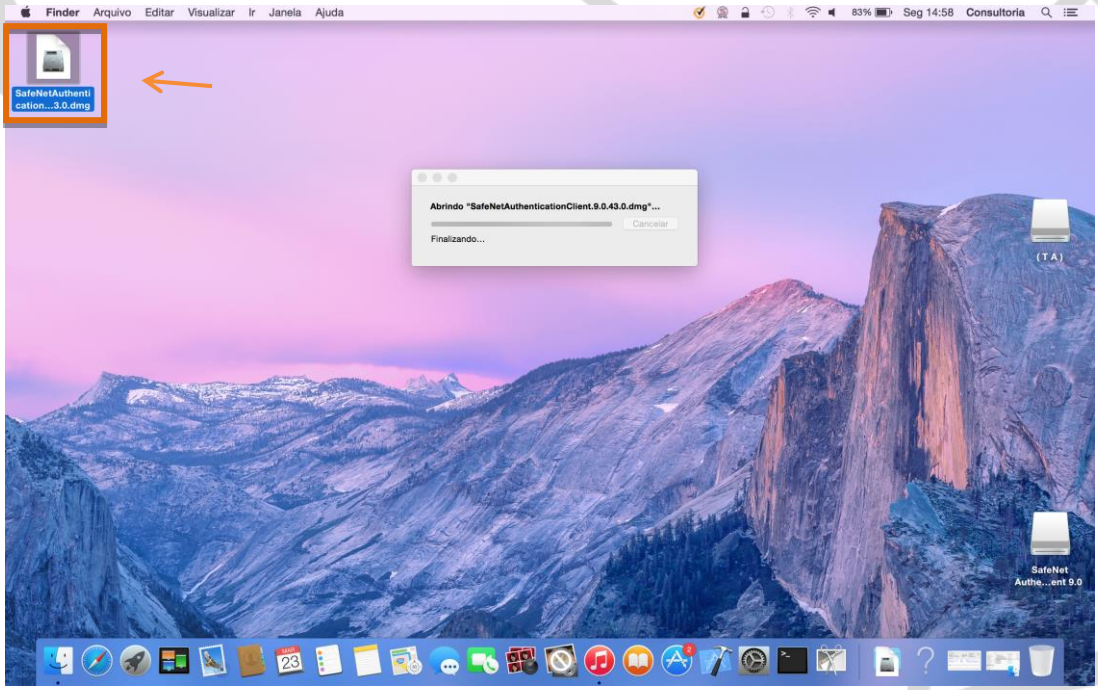


Figura 1 - Download do Pacote do SafeNet

Após o download do arquivo, o primeiro passo para instalação do SafeNet é descompactá-lo, para isso basta dar um duplo clique sobre o arquivo e o MAC OS realizará a descompactação automática do arquivo dentro da Mesa de Trabalho.

As informações contidas neste documento não podem ser reproduzidas sem a expressa permissão da Certisign.

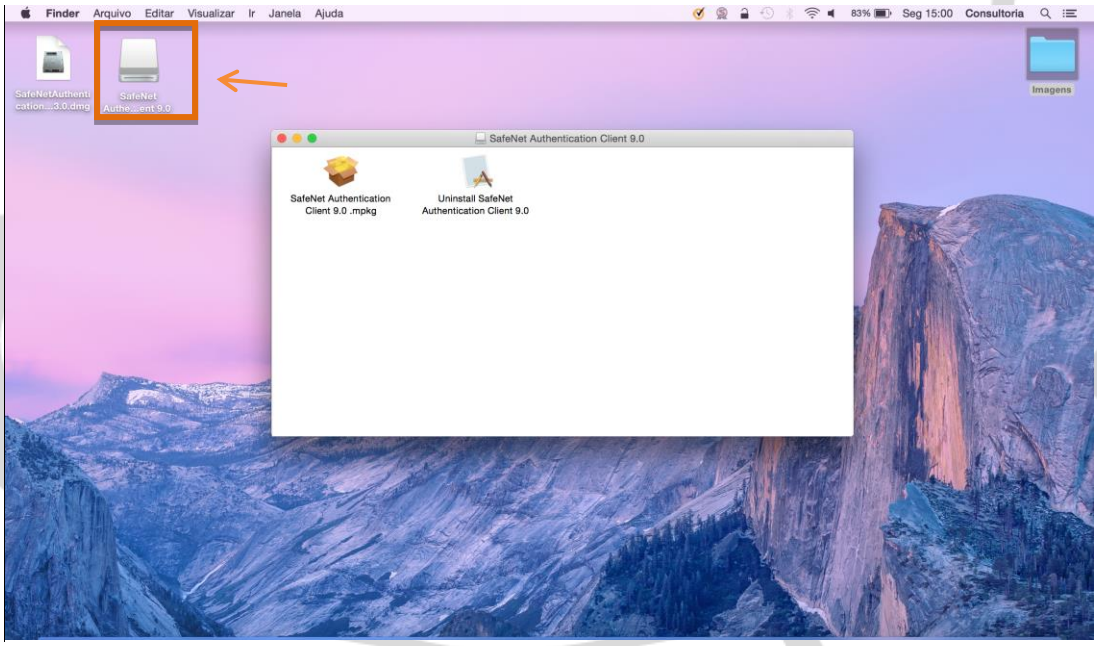


Figura 2 - Tela de com Safenet Descompactado

Para iniciar o processo de instalação é necessário clicar em: ***SafeNetAuthenticationClient 9.0.43.0.dmg***

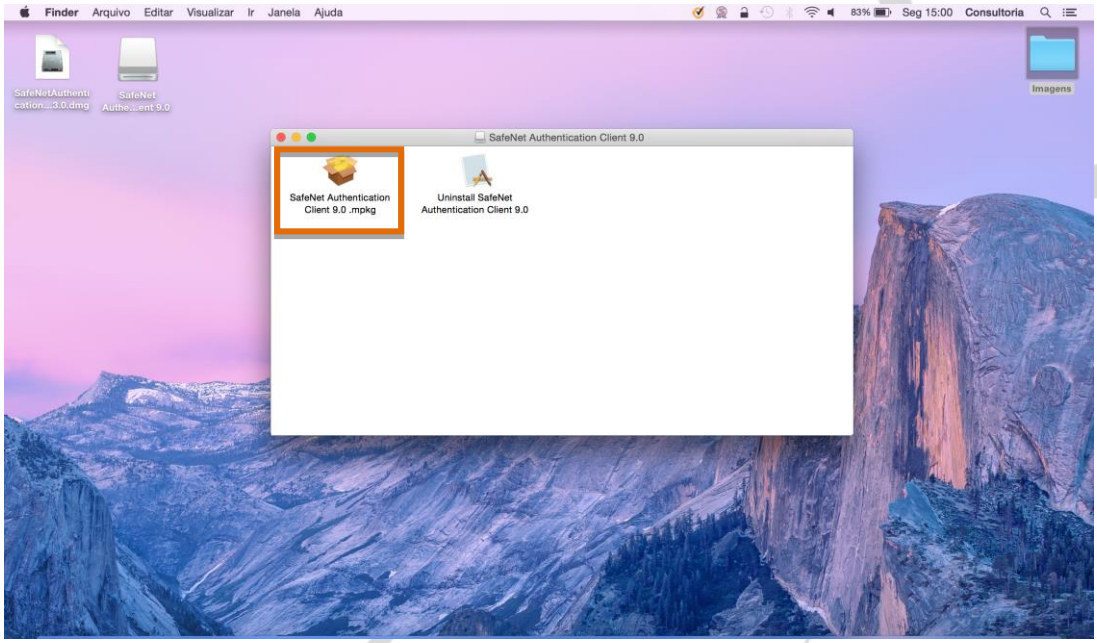


Figura 3 - Tela de com Safenet Descompactado

Para prosseguir com a instalação é necessário clicar sobre o botão **Continuar** do Instalador do SafeNet.

As informações contidas neste documento não podem ser reproduzidas sem a expressa permissão da Certisign.

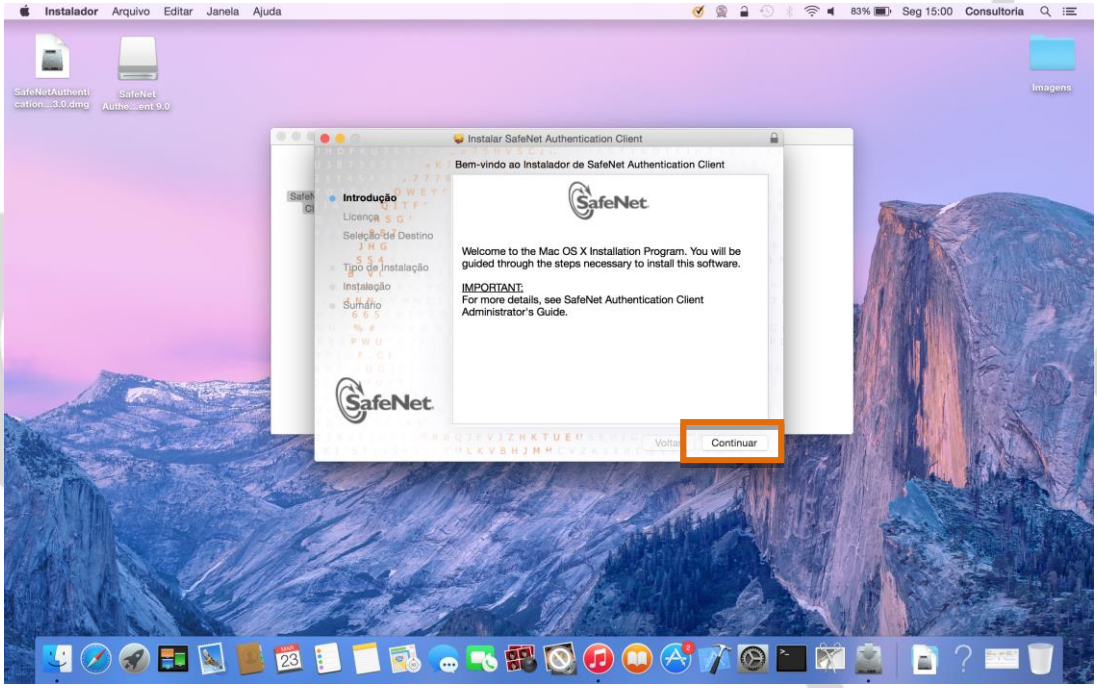

Instalador Arquivo Editar Janela Ajuda
Seg 15:00 Consultoria
Instalar SafeNet Authentication Client
Bem-vindo ao Instalador de SafeNet Authentication Client
Introdução
Licença
Seleção de Destino
Tipo de Instalação
Instalação
Sumário
Welcome to the Mac OS X Installation Program. You will be guided through the steps necessary to install this software.
IMPORTANT:
For more details, see SafeNet Authentication Client Administrator's Guide.
Voltar
Continuar

Figura 4 - Tela de Bem-Vindo do Instalador

Será apresentado contrato para utilização, conforme Figura 5.

Instalador Arquivo Editar Janela Ajuda
Seg 15:01 Consultoria
Instalar SafeNet Authentication Client
Licença de Uso de Software
English
Introdução
Licença
Seleção de Destino
Tipo de Instalação
Instalação
Sumário
SAFENET SOFTWARE LICENSE TERMS
SafeNet Authentication Client
Legal notice:
LICENSE AGREEMENT
IMPORTANT INFORMATION - PLEASE READ THIS AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE AND/OR USING THE CONTENTS THEREOF AND/OR BEFORE DOWNLOADING OR INSTALLING THE SOFTWARE PROGRAM. ALL ORDERS FOR AND USE OF SOFTWARE SUPPLIED BY SAFENET, INC. (or any of its affiliates - either of them referred to as "SAFENET") ARE AND SHALL BE, SUBJECT TO THE TERMS AND
Imprimir...
Salvar...
Voltar
Continuar

Figura 5 – Licença.

Clicar no botão “Continuar” e depois “Concordar”.

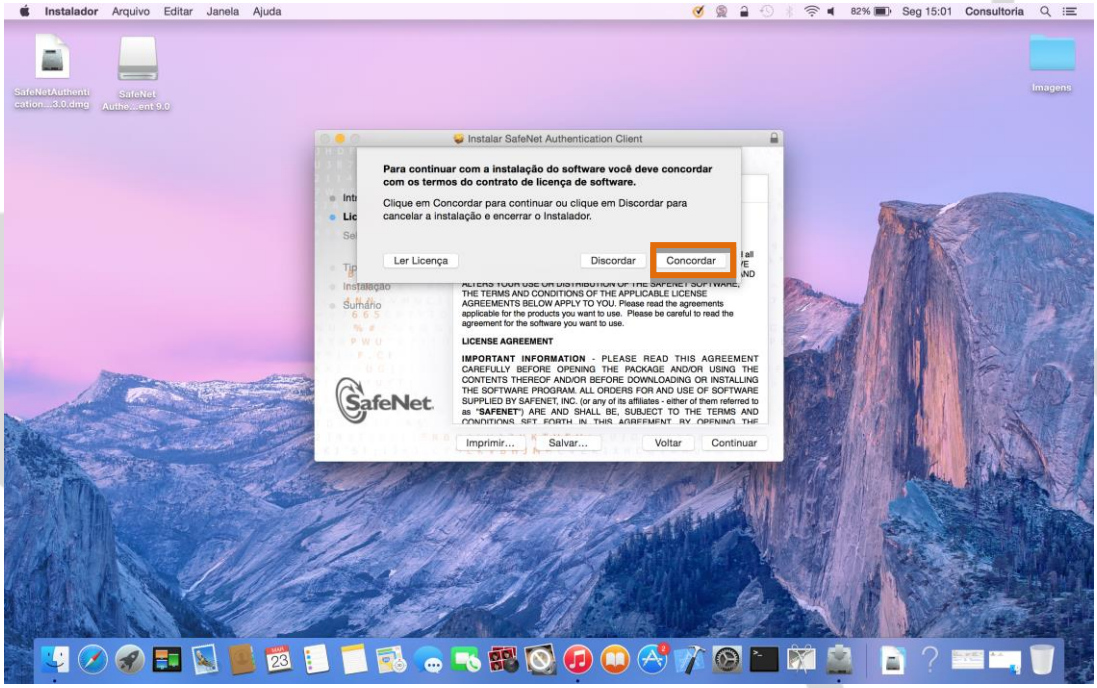

Instalador Arquivo Editar Janela Ajuda
Seg 15:01 Consultoria
Instalar SafeNet Authentication Client
Para continuar com a instalação do software você deve concordar com os termos do contrato de licença de software.
Clique em Concordar para continuar ou clique em Discordar para cancelar a instalação e encerrar o Instalador.
Ler Licença
Discordar
Concordar
LICENSE AGREEMENT
Imprimir...
Salvar...
Voltar
Continuar
Imagens

Figura 6 - Apresentação do Contrato

Neste momento será solicitado o usuário e senha com permissão de administração para que o processo de gravação dos arquivos seja gerado.

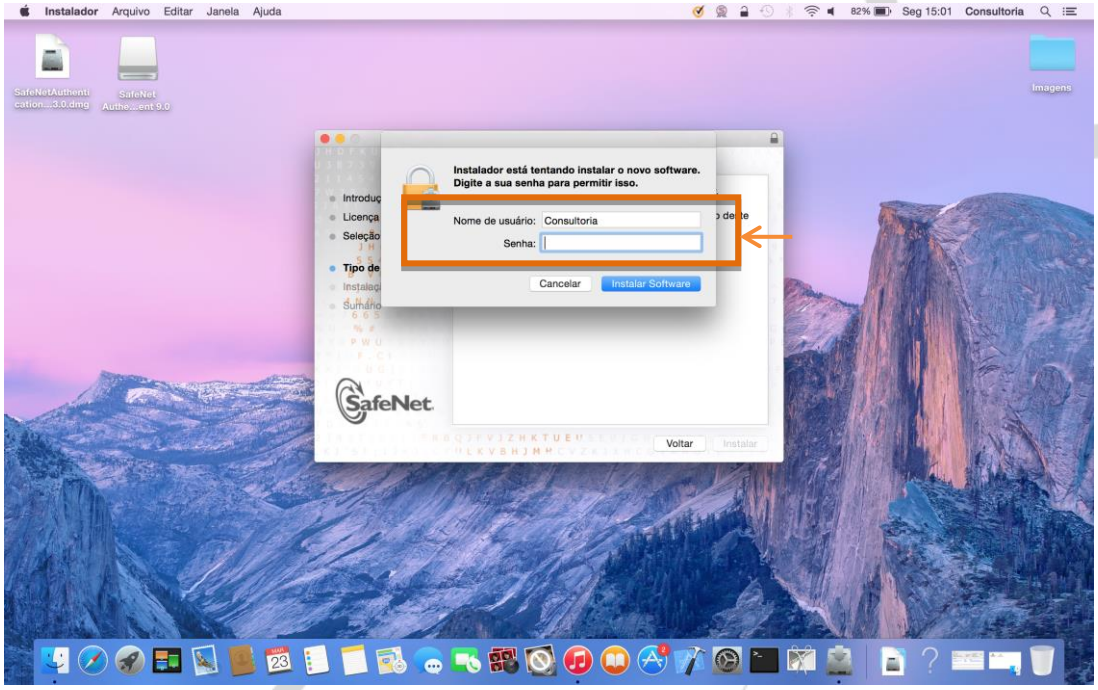


Figura 7 - Digitação das credenciais de acesso para instalação

Se você visualizou a tela apresentada na Figura 08 o processo de instalação foi completado com sucesso e seu computador MAC já possui a capacidade de entender as informações existentes dentro do Token.

Caso seja retornado alguma mensagem de erro o processo de instalação deve ser reiniciado.

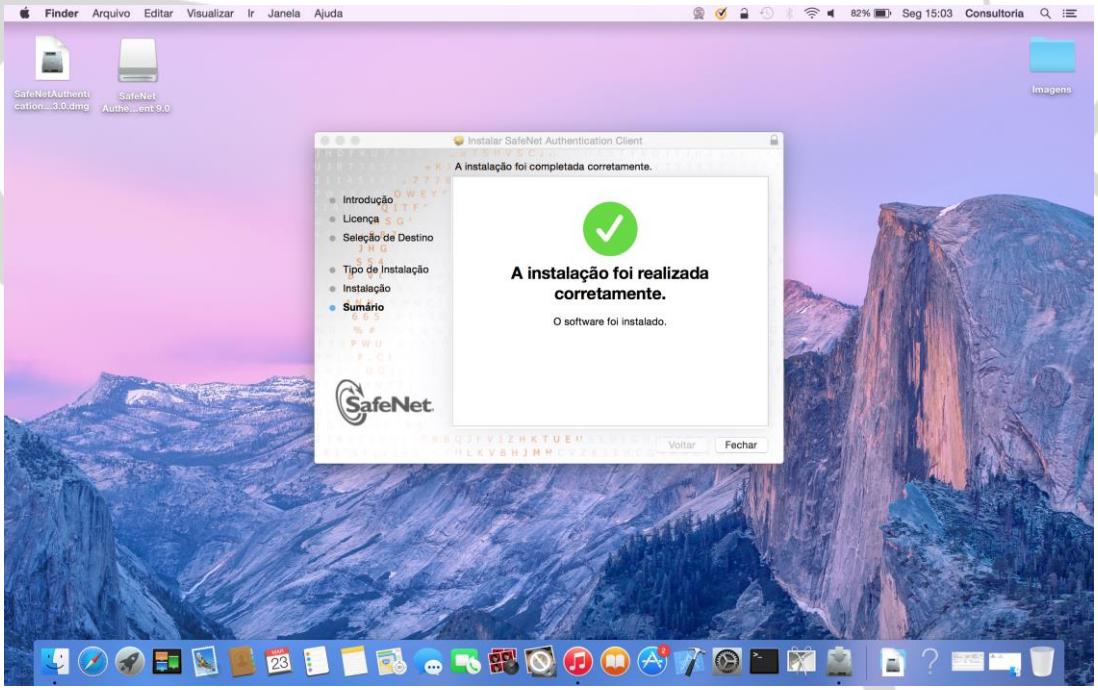


Figura 8 – Instalado com Sucesso.

4. Utilização do Certificado A3 no Navegador Mozilla Firefox 35.0.1.

Para utilizar seu certificado digital armazenado em uma mídia criptográfica na internet, através de seu computador MAC, recomendamos a utilização do navegador Firefox que utiliza a interface de conexão PKCS#11 e pode ser instalado através do site *http://www.mozilla.com.* (Versão 35.0.1.)

Após a instalação do Mozilla Firefox 35.0.1 é necessário configurá-lo para que ele se conectar a aplicação SafeNet, e assim permitir o uso do certificado digital na internet.

Ressalto que todo o procedimento realizado abaixo deve ser efetuado com a mídia conectada na máquina.

Abra o menu FIREFOX conforme a Figura 9:

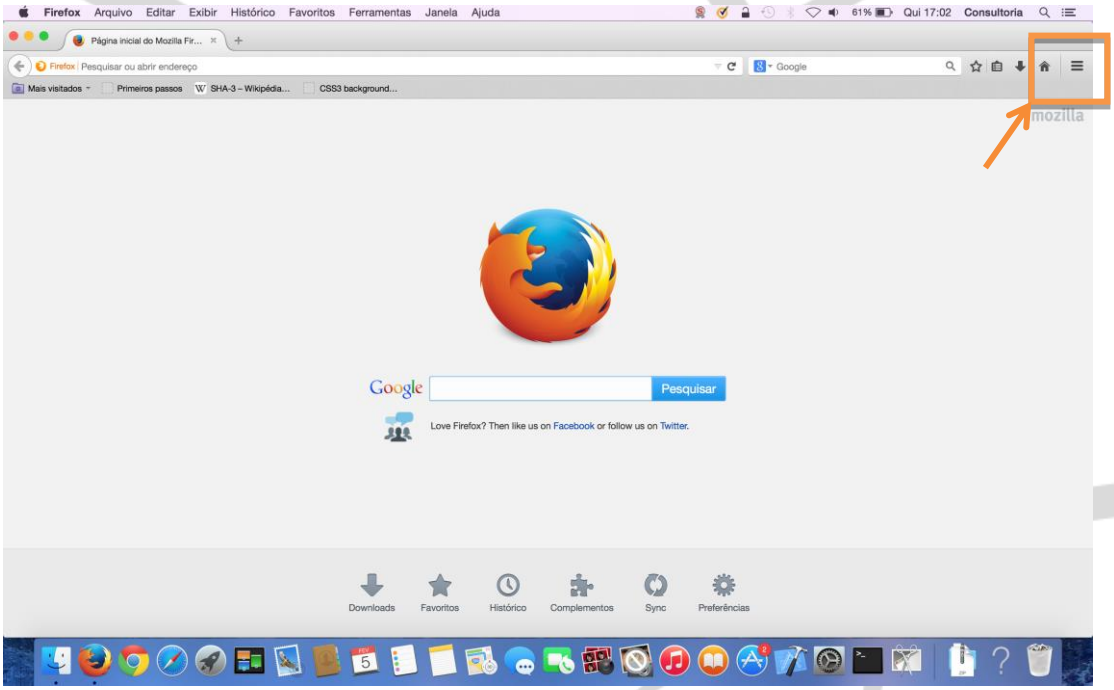


Figura 9 - Abertura do Menu Firefox

Clicar em Preferências conforme a figura 10.

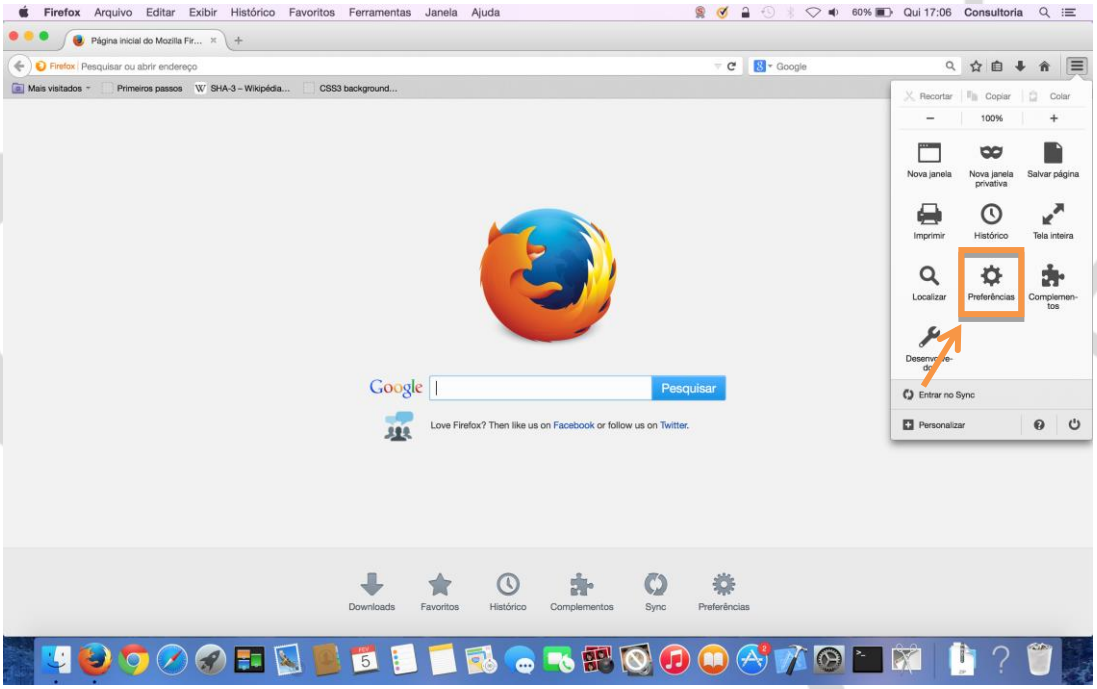


Figura 10 - Opções do Menu Firefox

Clicar sobre o botão "**Avançado**" como o passo 1 da Figura 11, logo em seguida clicar sobre a guia "**Criptografia**" como passo 2 da mesma figura e depois clicar sobre o botão "**Dispositivos de segurança**".

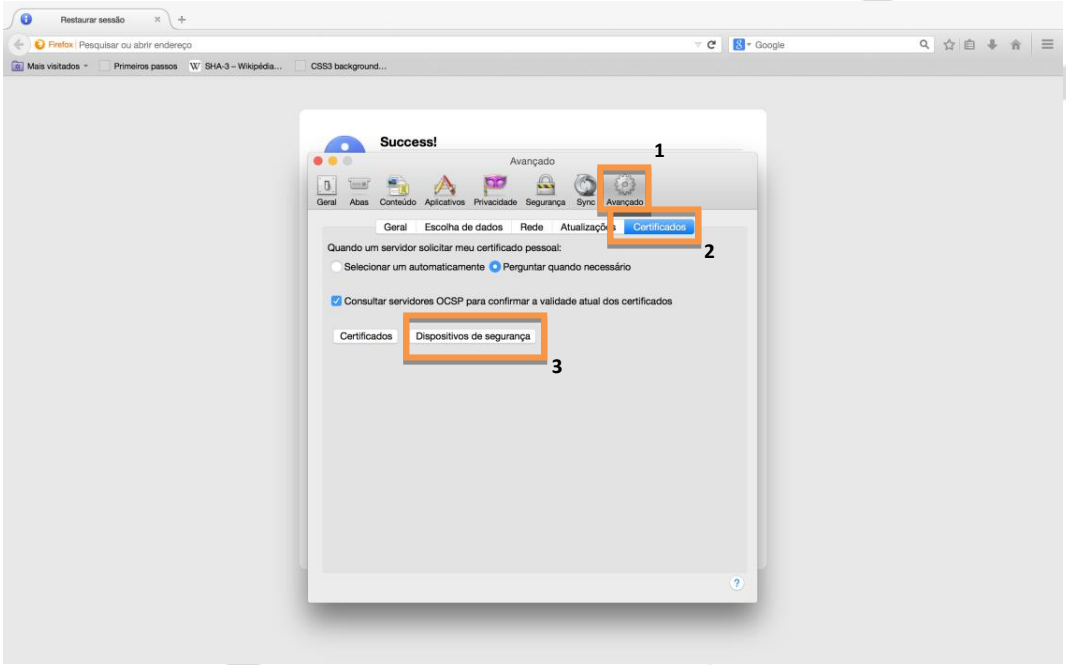


Figura 11 - Abertura dos Dispositivos de Segurança

As informações contidas neste documento não podem ser reproduzidas sem a expressa permissão da Certisign.

Será iniciado o Gerenciador de Dispositivos de Segurança. Neste momento é necessário configurar a conexão entre o Firefox e o Safenet, para isso é preciso que seja apontada a biblioteca que será utilizada pelo navegador.

Para iniciar o processo de configuração deve clicar no botão carregar conforme a Figura 12.

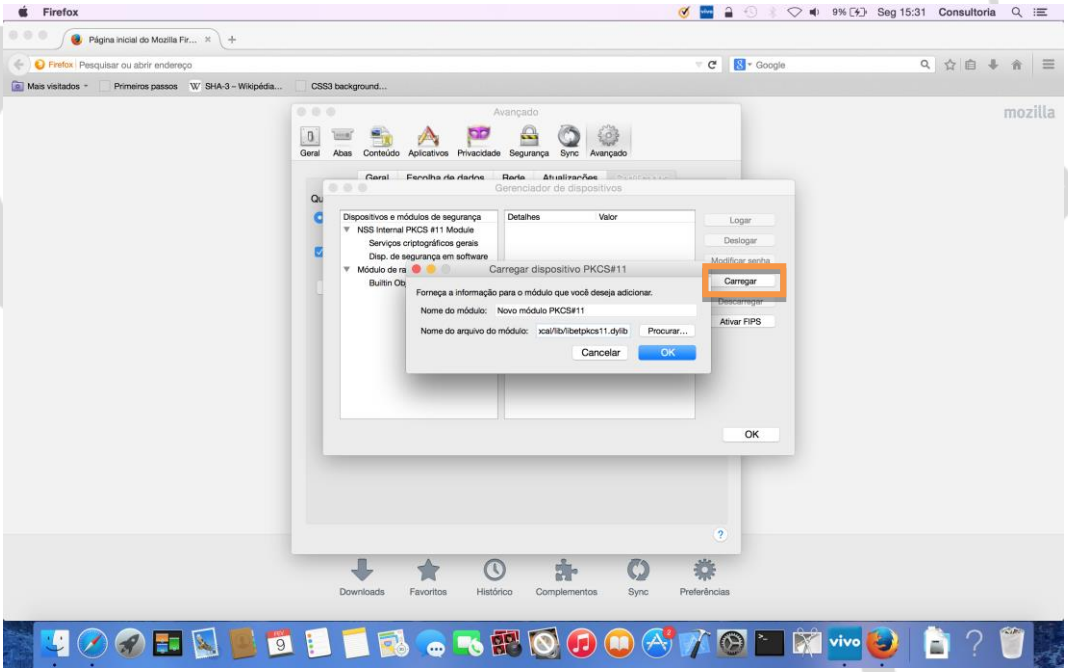


Figura 12 - Gerenciador de Dispositivos

Para carregar um novo dispositivo PKCS#11 é necessário informar um nome para esse dispositivo e preencher o campo “Nome do módulo”, conforme passo 1 da Figura 13.

Necessário que campo “Nome do arquivo do módulo” deve ser preenchido com o valor ***“/usr/local/lib/libetpkcs11.dylib”***.

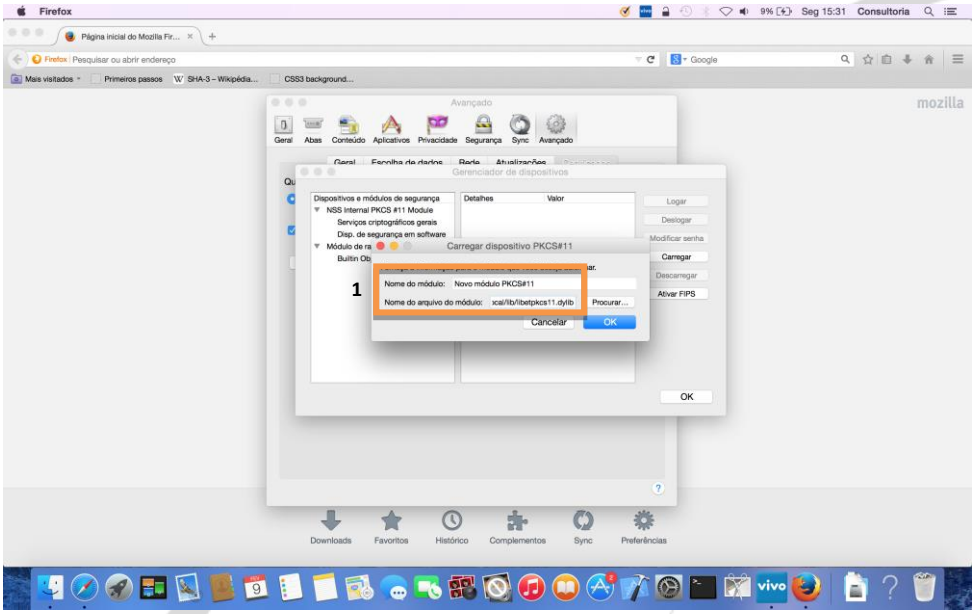


Figura 13 - Carregar dispositivo PKCS#11

As informações contidas neste documento não podem ser reproduzidas sem a expressa permissão da Certisign.

Uma vez que a biblioteca foi localizada um novo dispositivo criptográfico é carregado e apresentado na tela do Gerenciador de Dispositivos, caso aconteça algum erro é necessário verificar se os valores digitados no campo “Nome do arquivo do módulo” estão corretos ou se o Safenet está corretamente instalado.

Em caso de duvidas entrar em contato com SAC da Certisign.

Para verificar se o dispositivo foi corretamente carregado é necessário apenas analisar se dentro do Gerenciador de Dispositivos, na coluna da esquerda é apresentada uma nova linha com o texto cadastrado no campo “Nome do módulo” e se abaixo dessa linha é apresentado o nome do token ou o nome do label conectado, como mostra a Figura 14 e 15.

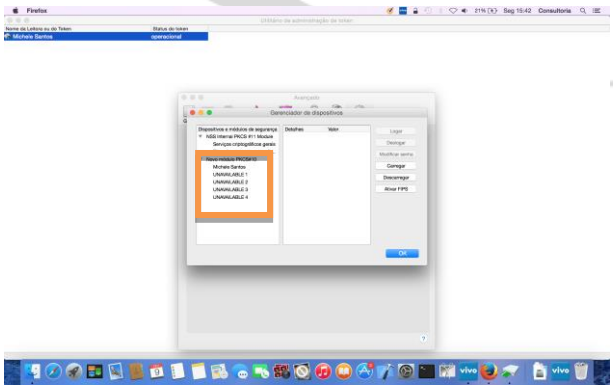


Figura 14 - Gerenciador de Dispositivos

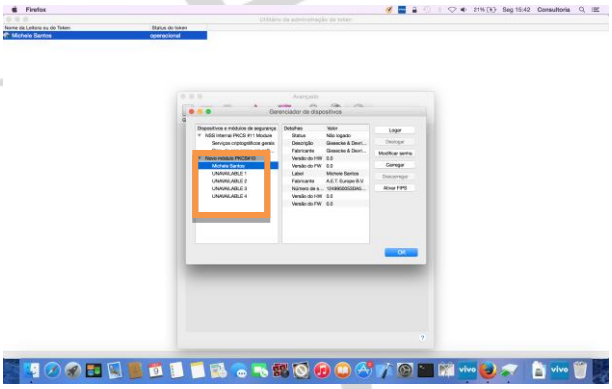


Figura 15 – Gerenciador de Dispositivos

Caso todos os passos tenham sido completados com sucesso, seu certificado armazenado em um token está pronto para se comunicar com Navegador Mozilla Firefox.

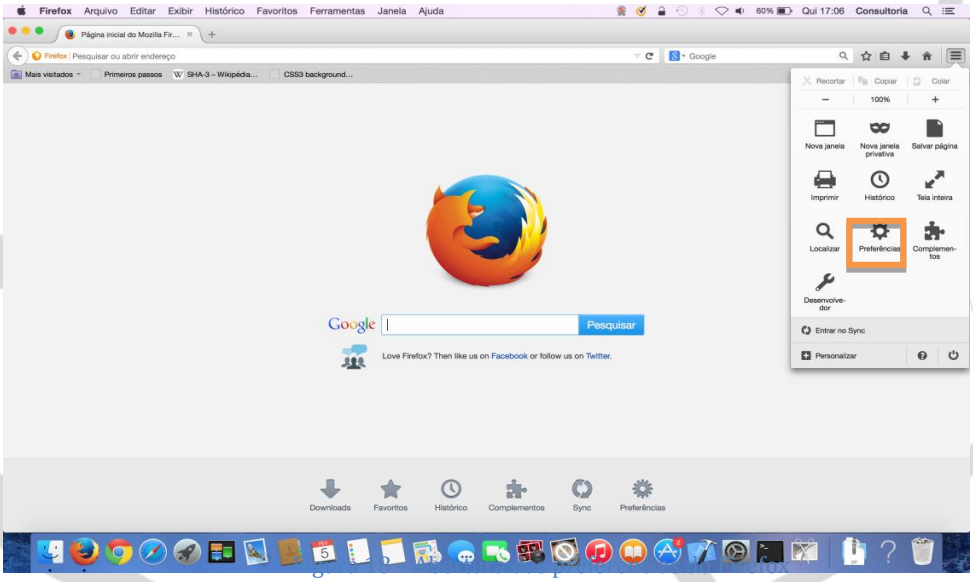
Para instalar as cadeias de certificação, você deve ir até o site da Autoridade Certificadora e baixar os arquivos contendo as cadeias.

(http://www.certisign.com.br/atendimento-suporte/downloads/hierarquias)

Esses arquivos possuem a extensão .CER e devem ser salvos na mesa de trabalho do seu Mac Osx.

Após realizar o download desses arquivos você deve abrir o menu FIREFOX e escolher a opção Preferências, como mostra a Figura 17.

As informações contidas neste documento não podem ser reproduzidas sem a expressa permissão da Certisign.



Serão abertas as abas de configurações do Firefox, escolha o botão **Avançado**, a guia **Criptografia** e botão **Certificados**. Será aberto o Gerenciador de Certificados escolha a Guia Autoridades e clique no botão Importar, como mostra a Figura 19.

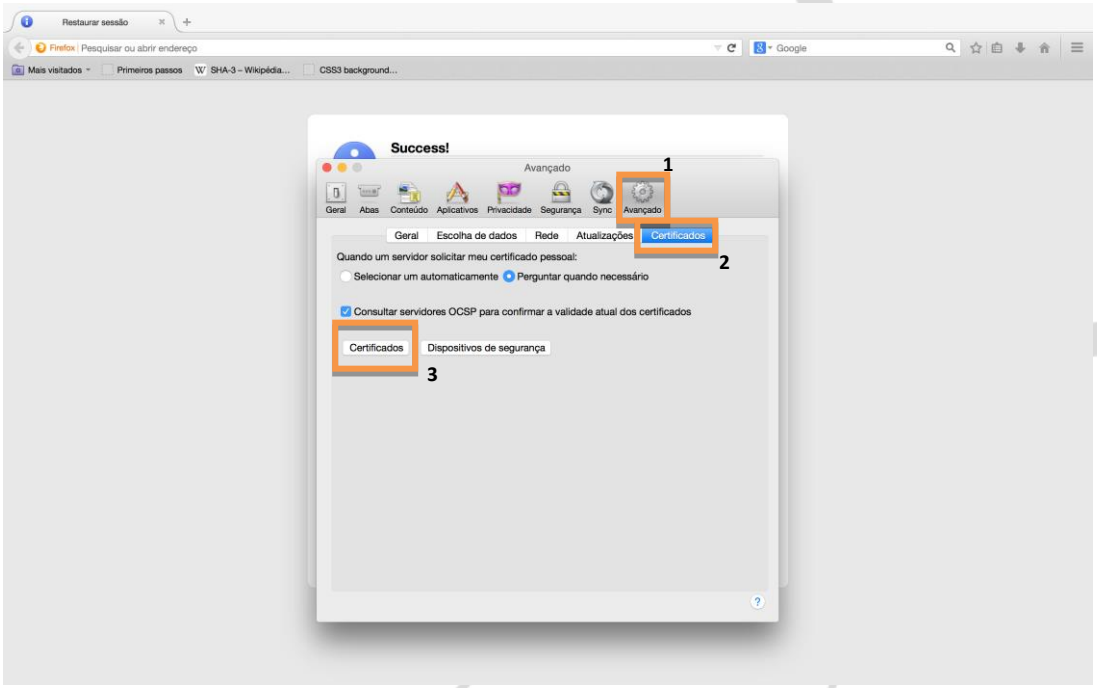
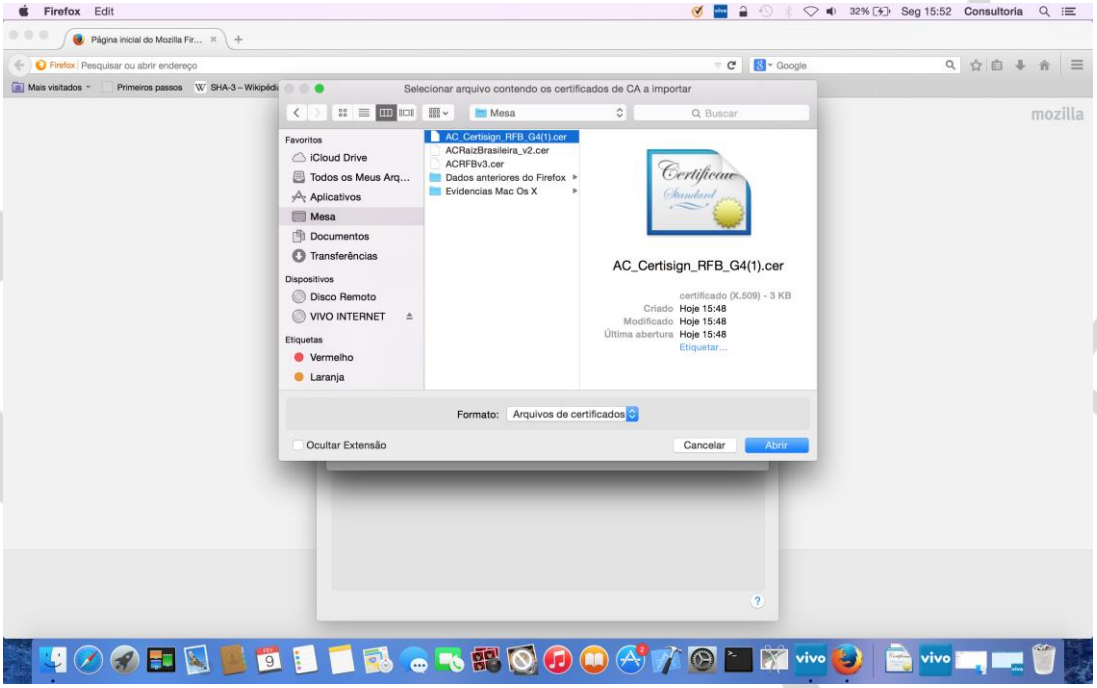


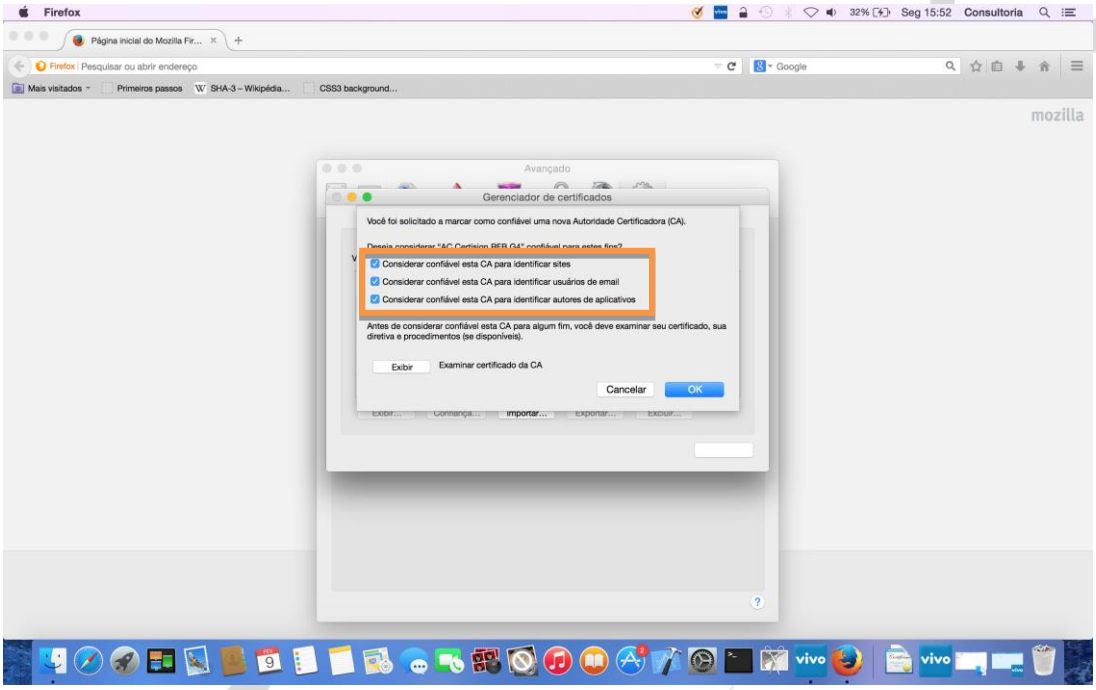
Figura 19 – Abertura das preferencias do Firefox

No botão importar de arquivos selecione os arquivos que compõem as cadeias de certificados que foram baixadas no site da Autoridade Certificadora. É necessário que antes que cada cadeia seja habilitada as três opções de confiança:



Selecione as 3 opções descritas abaixo ao importar a hierarquia para o Navegador Mozilla Firefox:

- O Certificado pode identificar sites
- O Certificado pode identificar usuários de email
- O Certificado pode identificar desenvolvedores de aplicativos


Gerenciador de certificados
Você foi solicitado a marcar como confiável uma nova Autoridade Certificadora (CA).
Considerar confiável esta CA para identificar sites
Considerar confiável esta CA para identificar usuários de email
Considerar confiável esta CA para identificar autores de aplicativos
Antes de considerar confiável esta CA para algum fim, você deve examinar seu certificado, sua diretiva e procedimentos (se disponíveis).
Exibir
Examinar certificado da CA
Cancelar
OK

Repita o procedimento com todas as hierarquias correspondentes ao certificado digital.

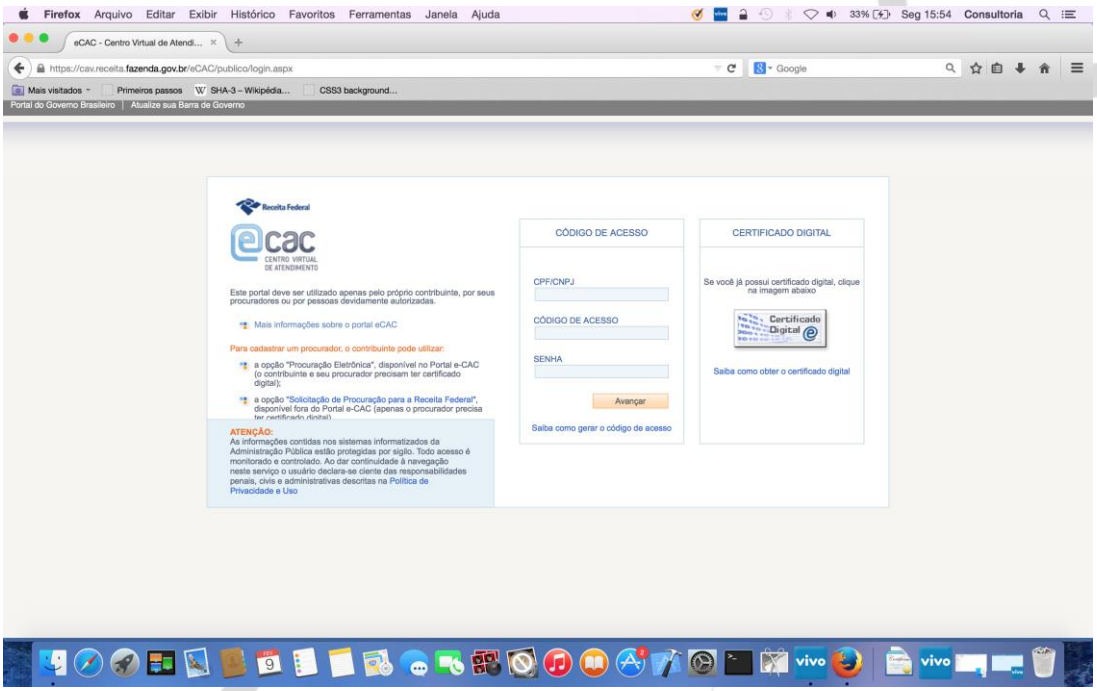
As informações contidas neste documento não podem ser reproduzidas sem a expressa permissão da Certisign.

5. Teste o Certificado Digital.

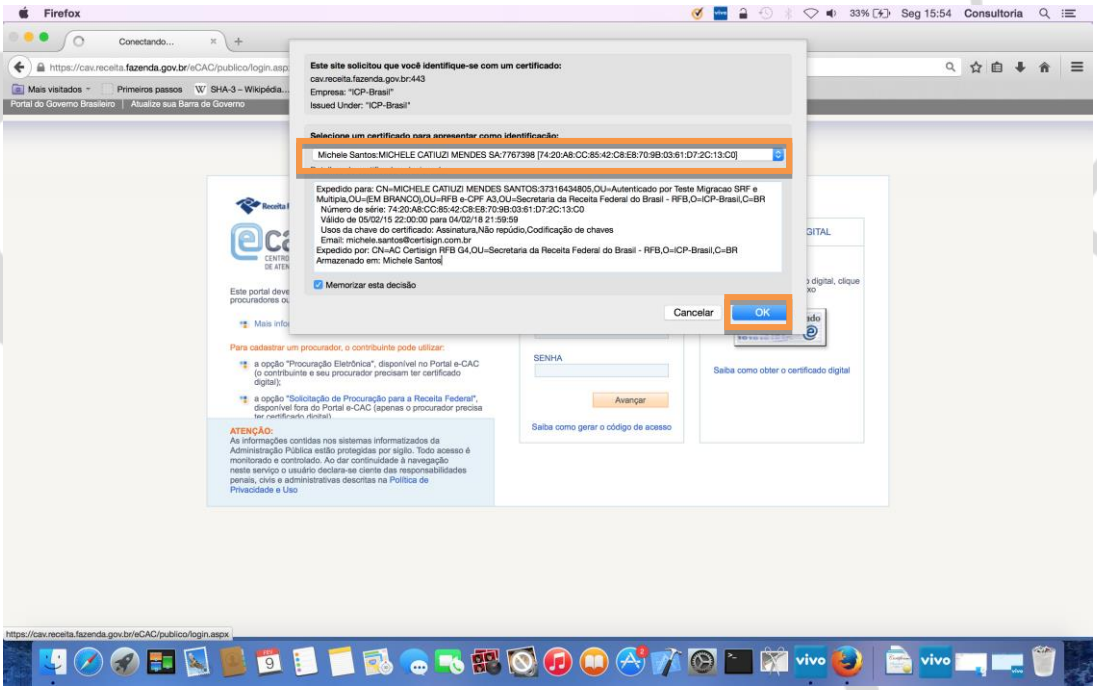
Para verificar o funcionamento do seu certificado, acesse o site da Receita Federal do Brasil (http://idg.receita.fazenda.gov.br/) através do Navegador Mozilla Firefox.

Selecione a opção "Atendimento Virtual (e-CAC)"

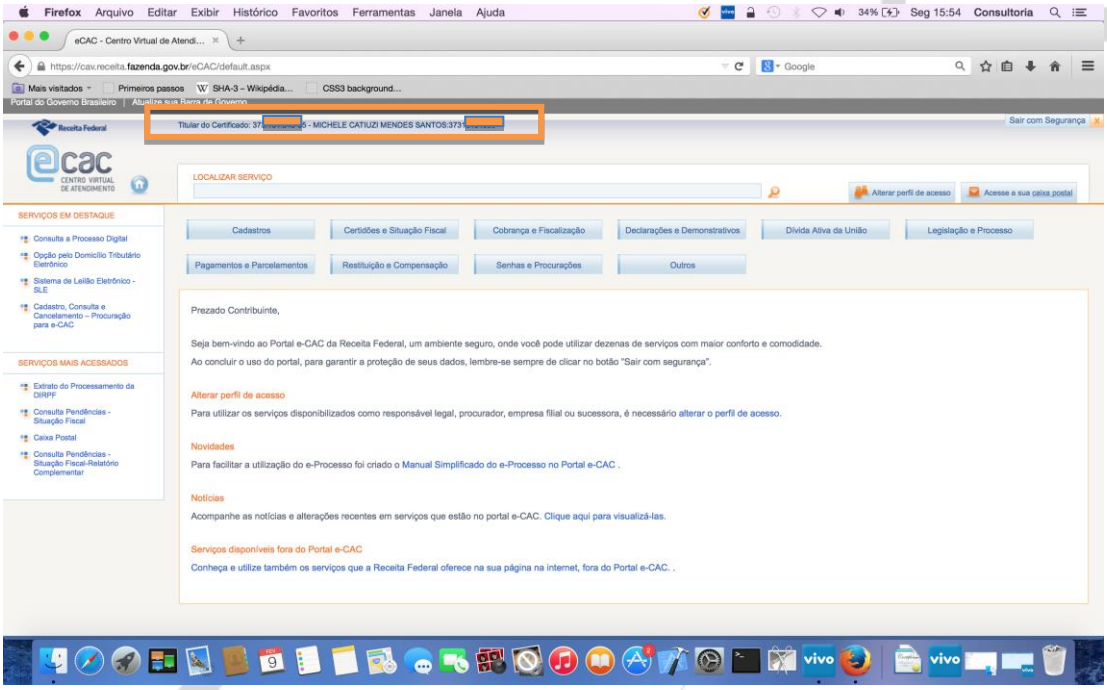
Selecione a opção **"Certificado Digital"**


Firefox
Arquivo
Editar
Exibir
Histórico
Favoritos
Ferramentas
Janela
Ajuda
Seg 15:54
Consultoria
eCAC - Centro Virtual de Atendi...
https://cav.receita.fazenda.gov.br/eCAC/publico/login.aspx
Receita Federal
eCAC
CENTRO VIRTUAL DE ATENDIMENTO
Este portal deve ser utilizado apenas pelo próprio contribuinte, por seus procuradores ou por pessoas devidamente autorizadas.
Mais informações sobre o portal eCAC
Para cadastrar um procurador, o contribuinte pode utilizar:
a opção "Procuração Eletrônica", disponível no Portal e-CAC (o contribuinte e seu procurador precisam ter certificado digital);
a opção "Solicitação de Procuração para a Receita Federal", disponível fora do Portal e-CAC (apenas o procurador precisa ter certificado digital).
ATENÇÃO:
As informações contidas nos sistemas informatizados da Administração Pública estão protegidas por sigilo. Todo acesso é monitorado e controlado. Ao dar continuidade à navegação neste serviço o usuário declara-se ciente das responsabilidades penais, civis e administrativas descritas na Política de Privacidade e Uso
CÓDIGO DE ACESSO
CPF/CNPJ
CÓDIGO DE ACESSO
SENHA
Avançar
Saiba como gerar o código de acesso
CERTIFICADO DIGITAL
Se você já possui certificado digital, clique na imagem abaixo
Certificado Digital
Saiba como obter o certificado digital

Verifique se o certificado que aparece é o mesmo certificado correspondente a mídia criptográfica conectada na maquina, selecione o mesmo e clique em OK.



Será apresentada uma tela de boas vindas ao Portal e-CAC da Receita Federal. Certifique-se que as informações apresentadas no topo do site são correspondentes ao certificado digital utilizado.


Prezado Contribuinte,
Seja bem-vindo ao Portal e-CAC da Receita Federal, um ambiente seguro, onde você pode utilizar dezenas de serviços com maior conforto e comodidade.
Ao concluir o uso do portal, para garantir a proteção de seus dados, lembre-se sempre de clicar no botão "Sair com segurança".
Alterar perfil de acesso
Para utilizar os serviços disponibilizados como responsável legal, procurador, empresa filial ou sucessora, é necessário alterar o perfil de acesso.
Novidades
Para facilitar a utilização do e-Processo foi criado o Manual Simplificado do e-Processo no Portal e-CAC .
Notícias
Acompanhe as notícias e alterações recentes em serviços que estão no portal e-CAC. Clique aqui para visualizá-las.
Serviços disponíveis fora do Portal e-CAC
Conheça e utilize também os serviços que a Receita Federal oferece na sua página na internet, fora do Portal e-CAC. .

Seu certificado digital está pronto para uso: caso contrário, realize novamente o procedimento de instalação. Se o erro persistir, entre em contato com o Serviço de Atendimento ao Cliente (SAC).

São Paulo: 3478-9444 / Demais localidades: 0300-789-2378
Email: sac@certisign.com.br
Segunda à sexta-feira, das 8h às 20h (exceto feriados nacionais)
www.certisign.com.br

Criado por: Michele Catiuze Mendes Santos

Qualidade e Segurança de Software

São Paulo, 23 de Março de 2015.

As informações contidas neste documento não podem ser reproduzidas sem a expressa permissão da Certisign.